## Ifconfig Lab 1: Network & Protocols

Intro IT & Web Science - ITWS 1100

The purpose of this lab is to get you familiar with some basic networking concepts, protocols, and tools. We will start the lab in class. Please enter your answers in this document and save it as “Lab1-*YourFullName.docx*”. It is due in the Assignment area by EoD on the next class-day.

1. **Basic Network Information**For the following exercises, open a “Command Prompt” console window on your laptop, enter each command as shown on the command line, and answer the questions provided. To copy from the Command Console, block text with your mouse and right-click or hit enter. (If you cannot block text directly, right-click and select “Mark” first). If you are using Linux/Unix/OS X, perform the equivalent command (shown in parentheses) in a terminal window.

**Hint:** Read about Netstat (you can also search this site for other info ie ipconfig) for Windows here: <https://technet.microsoft.com/en-us/library/bb490947.aspx>

**Hint:** Mac info is here: <https://developer.apple.com/library/archive/documentation/System/Conceptual/ManPages_iPhoneOS/man3/getifaddrs.3.html>

**Hint:** If you are having issues retrieving IPv6 or v4 info from the commands – look up the options for ipconfig, etc

* 1. **ipconfig /all** (Windows)

**ifconfig –a** and **scutil --dns**, and **netstat -nr | grep default** (Mac)

(Also on Mac – AppleMenu->About->MoreInfo->System report, ifconfig en1)

(can also type hostname from the command line –mac/linux)

For your LAN Ethernet adapter and your general IP configuration:

* + 1. What is your hostname?

CallumXPS

* + 1. What is your MAC address?

9C-B6-D0-B8-5E-D3

* + 1. Who is the vendor of your Ethernet adapter?

Killer

* + 1. What is your IPv4 address?

129.161.49.181

* + 1. What is your IPv6 address?

fe80::1df3:e1ec:3bf6:b197

* + 1. What are the IP (v4) addresses of your DNS servers?

128.113.26.250

128.113.28.68

* + 1. What is the IP (v4) address of your default gateway

129.161.49.254

* 1. **netstat –f** (netstat –f inet)
     1. What kind of transport layer protocols are in use?

TCP

* + 1. What kind of application layer protocols are in use?

HTTP and HTTPS

* 1. **netstat –b** (netstat –b –f inet)
     1. What applications are using your network ports, and what application layer protocol are they using? (only name up to three)   
        chrome.exe port: 1024 and more protocol: TCP

OfficeClickToRun.exe port: 1043 protocol: TCP

OriginWebHelperService.exe port: 1027 protocol: TCP

* 1. **nslookup 192.0.32.10**nslookup it allows you to look up IPs or hostnames against a name server (by default, the first DNS server configured in your network settings).
     1. Upon running “nslookup 192.0.32.10”, what is the host name of the name server you are using?

defiant.net.rpi.edu

* + 1. What name is associated with 192.0.32.10? What is the significance of this name?

ICANN, which is the Internet Corporation for Assigned Names and Numbers. They coordinate and provide maintenance/procedures related to namespaces of the Internet.

* + 1. Perform a “netstat –n” in your console (this tells netstat not to resolve names against the name server – notice that it’s quicker). Do an nslookup on a foreign IP from your netstat results. What name did you uncover? (If the DNS server can’t resolve the IP you picked, try another one.)

Running nslookup 185.199.111.133 resulted in cdn-185-199-111-133.github.com

* + 1. Do an “nslookup 127.0.0.1”. What name is returned? What is the significance of this name?

Localhost is returned. This is significant because 127.0.0.1 is the loopback address and should send all traffic back to my computer, which is localhost.

* + 1. What is the IP address of lms.rpi.edu?

There are 4 IP addresses (4 servers):

18.204.171.76

35.172.47.233

34.227.233.206

3.221.129.40

* + 1. What is the IP address of www.rpi.edu? Is it IPv4 or IPv6?

2620:0:2820:4::2 and 128.113.0.2. It has both an IPv4 and an IPv6 address.

* 1. **tracert www.ucla.edu** (traceroute www.ucla.edu)
     1. How many hops did it take for you to reach [www.ucla.edu](http://www.ucla.edu/)?

14 hops

* + 1. From the tracert you just ran, locate an IPv4 address of a router along the path. Visit <http://www.iplocation.net/> and enter the IPv4 address. Were you able to determine the router’s location? If so, where is it?

162.252.70.131 → Ann Arbor, Michigan

* + 1. Enter your own IPv4 address in the website. What did you learn?

The location is Troy, New York (obviously), and Rensselaer Polytechnic Institute is considered the ISP. Anyone who has my IP (all servers I connect to) know approximately where I am, but each of the location services gives a slightly different latitude and longitude.

1. **SSH to RCS-Linux**

For this exercise you are going to create a terminal session onto another computer and run some network commands there.

Read up on

* SSH: <https://www.ssh.com/ssh/protocol/>
* And how to use it on Windows; [Here](https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/ssh-remoting-in-powershell-core?view=powershell-7) or [here](https://docs.microsoft.com/en-us/windows/terminal/tutorials/ssh).
* On Mac or Unix you can use the normal terminal

If you are off-campus, you will need the VPN active on your computers; While it should be pre-loaded on your laptops from RPI already, you can find out more about it here

<https://itssc.rpi.edu/hc/en-us/articles/360008783172-VPN-Installation-and-Connection>

Use SSH to *yourRCSid@***rcs-linux.rpi.edu** (for those on Linux/Unix/OS X, ssh directly from your terminal). Log in with your RCS ID and password. You will arrive in your Rensselaer Computing System (RCS) home directory.

NOTE: If you are off-campus, you must connect to RPI’s VPN (Virtual Private Network) to access rcs-linux.rpi.edu. This is accomplished by running a VPN client on your system such as the “Cisco AnyConnect VPN client” which is likely installed on your laptop already. For instructions on how to get the VPN client and information about VPN access, please see: <http://helpdesk.rpi.edu/update.do?artcenterkey=556>

* 1. **netstat -e**
     1. What transport layer protocols do you see in use?

TCP and TCP6

* + 1. What application layer protocols do you see in use?

HTTP and HTTPS

* 1. **host www.rpi.edu**
     1. What IPv4 addresses are used by [www.rpi.edu](http://www.rpi.edu/)?

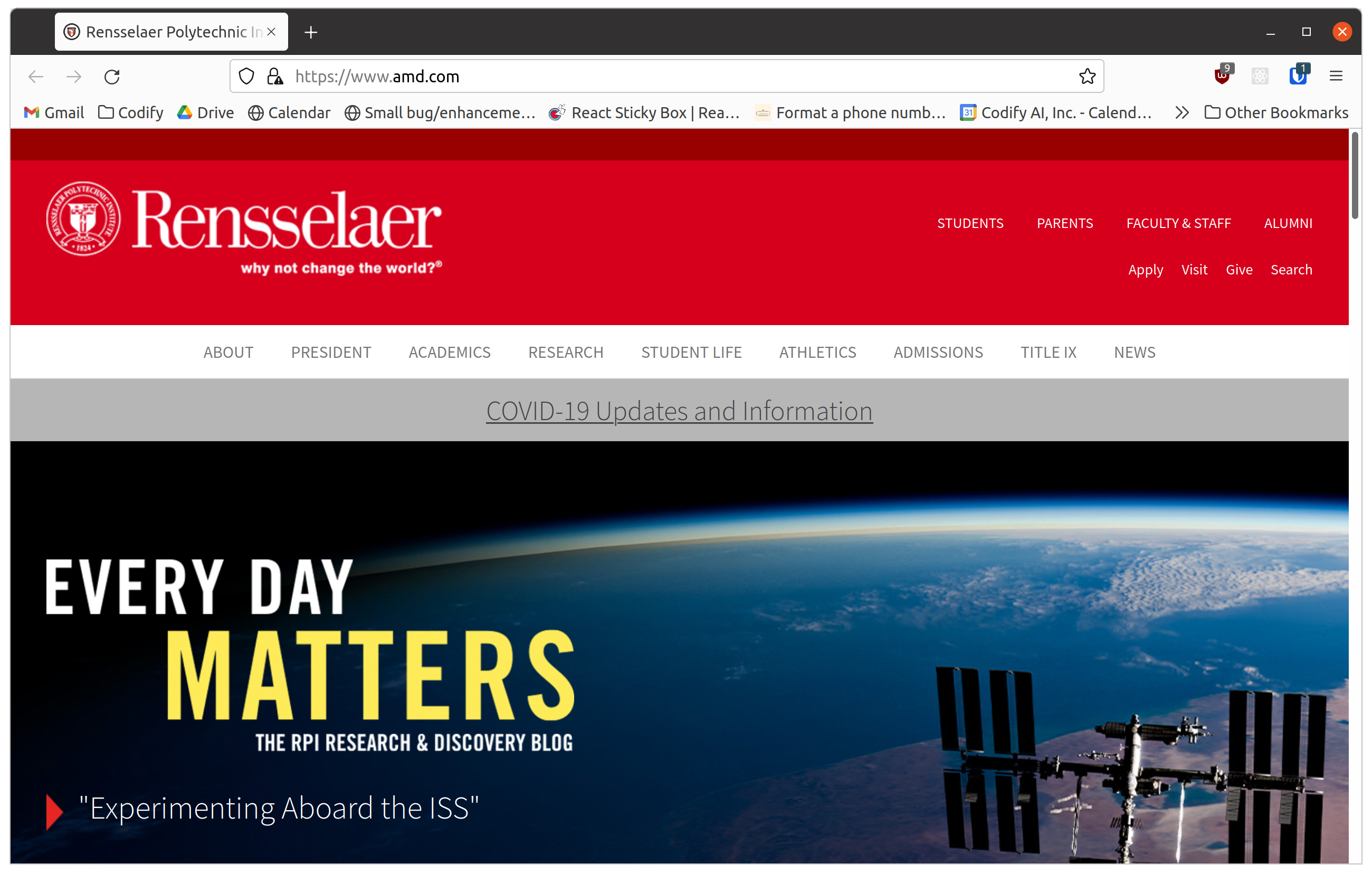
128.113.0.2

* 1. **traceroute www.google.com**
     1. How many hops did it take to get to Google?   
        9
  2. In your Windows Command Prompt console use netstat (as in section 1.b) to find your current SSH connection. Mac users : Use command **who -a** as well as **netstat**

Copy the netstat line showing the SSH connection to here.

tcp6 0 0 callum-ubuntu:33028 rmtacc-r7c.rcs.rpi.:ssh ESTABLISHED

1. **Overriding DNS**Your machine has a local “hosts” file that maps IP addresses to host names and can be used to override DNS. (On some browsers, esp Chrome – the DNS information can be cached. Before and after this exercise, you should go into your browser’s settings and empty your cache.)
   1. Use jEdit, notepad or some other text editor to edit your hosts file: C:\Windows\System32\drivers\etc\hosts (/etc/hosts on linux/unix). Using the examples in the comments at the top of the hosts file as a guide, give www.rpi.edu a new host name – you can use any IP address of www.rpi.edufor this exercise (you need only one IP).
   2. Visit the new hostname in your browser and capture a screenshot of the browser window. (CTRL-SHIFT-ALT PrntScrn)
   3. Paste the screenshot here.



* 1. (I’d encourage you to now return your hosts file to its original state. Then clear your Browser’s cache).)

1. Do one of the following – or both if you’re bored.
   1. **(OPTION A – For those who are like – “I love this networking stuff”) Take a look at some packets**  
      Download and install WireShark: <http://www.wireshark.org/download.html>  
      There are ports of this for most OSes – if you’re not running Windows or Mac, scroll down on the Download page and look to the right. *(Note: I encourage you to run this only against your own machines. Also note that activities such as port scanning against RPI network devices will be noticed…)*
      1. Run WireShark and select “Capture Options, start a capture with detailed options”.
         1. Set the Capture Filter to “tcp port 80” (or “tcp port http”)
         2. Set “Stop Capture after **4** packets”
         3. Click “start”
      2. In your browser, visit <http://rpi.edu/>
         1. Looking back at the WireShark output, look for the TCP three-way handshake.
      3. How are the SYN and ACK flags represented in the TCP header? (Feel free to investigate <http://en.wikipedia.org/wiki/Transmission_Control_Protocol> as well.)

SYN and ACK flags are represented as 1 bit values in the flags section of the TCP header. The flags section is 9 bits and TCP header itself is represented as a set of 20 bytes (or octets).

* + 1. Look at the HTTP Request header. Copy your user-agent here (right-click to copy).

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:91.0) Gecko/20100101 Firefox/91.0